ЭКСПЕРТНОЕ ОЦЕНИВАНИЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ В БАЗЕ ДАННЫХ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Алексеев В.В.[1], Дидрих В.Е.[2], Белевитин В.А.[3], Дерябин А.С.[4]

Ключевые слова: *информационная система, база данных, привилегированная информация, защищенность, несанкционированный доступ, экспертная оценка, достоверность, оперативность, веб-приложение, методические рекомендации, коэффициент конкордации, экспертная информация.*

Аннотация

Цель работы: повысить достоверность и оперативность экспертного оценивания защищенности привилегированной информации от несанкционированного доступа в базе данных информационной системы.

Методы исследования: системный анализ, математическое и компьютерное моделирование, экспертное оценивание, программирование.

Результаты: разработаны методические рекомендации по анализу экспертных оценок защищенности информации от несанкционированного доступа в базе данных информационной системы с учетом требований нормативных правовых актов в сфере информационной безопасности; разработанная компьютерная программа и обоснованный порядок проведения экспертного оценивания обеспечивают его необходимую достоверность за счет устранения нерелевантных оценок экспертов, имеющих низкие значения коэффициента конкордации; использование экспертных анкет в веб-приложении, позволяющее уменьшить время от постановки задачи до выполнения ее экспертом, а также автоматизация процессов сбора и обработки экспертной информации позволяют также повысить оперативность экспертной оценки защищенности информации.

EDN: XNKLBE

Введение

В настоящее время *своевременное* получение *достоверных* экспертных оценок *защищенности* [12] информации от несанкционированного доступа (НСД) в базе данных информационной системы представляется особенно актуальным по следующим причинам.

1. *Увеличение угроз кибербезопасности.* Современные информационные системы сталкиваются с растущими угрозами кибербезопасности, такими как хакерские атаки, вредоносное программное обеспечение, киберпреступления и др. [5, 7]. Базы данных, содержащие привилегированную (ценную) информацию, становятся приоритетными целями для злоумышленников. Оценка степени защищенности информации позволяет идентифицировать уязвимости и риски, связанные с базой данных PostgreSQL, и предпринять соответствующие меры по укреплению ее безопасности. Кроме того, современное состояние развития и использования сетевых технологий на базе совершенной импортной компьютерной техники обеспечивает возможность осуществления НСД по *«нетрадиционным информационным каналам»* (*скрытым, англ. covert channel*), «невидимым» для современных средств защиты информации[5] [15, 16] даже при условии использова-

[5] См.: ГОСТ Р 53113.1-2008. Информационная технология. Защита ИТ и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. М. : Стандартинформ, 2008; ГОСТ Р 53113.2-2009. Информационная технология. Защита ИТ и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, ИТ и АС от атак с использованием скрытых каналов. М. : Стандартинформ, 2009.

[1] ***Алексеев Владимир Витальевич,*** *доктор технических наук, профессор, заведующий кафедрой информационных систем и защиты информации Тамбовского государственного технического университета, г. Тамбов, Российская Федерация.*

E-mail: vvalex1961@mail.ru

[2] ***Дидрих Валерий Евгеньевич,*** *доктор технических наук, профессор, профессор кафедры информационных систем и защиты информации Тамбовского государственного технического университета, г. Тамбов, Российская Федерация.*

E-mail: dve54@mail.ru

[3] ***Белевитин Виктор Андреевич,*** *аспирант кафедры информационных систем и защиты информации Тамбовского государственного технического университета, г. Тамбов, Российская Федерация.*

E-mail: adamunt@mail.ru

[4] ***Дерябин Андрей Сергеевич,*** *кандидат технических наук, доцент кафедры информационных систем и защиты информации Тамбовского государственного технического университета, г. Тамбов, Российская Федерация.*

E-mail: 799980@mail.ru

Таблица 1

Результат обобщения правовых особенностей проведения экспертной оценки

№	Наименование	Содержание
1	Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	Основные положения о защите информации, включая требования к проведению экспертизы информационной безопасности
2	Постановление Правительства РФ от 15 июля 2022 г. № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)»	Порядок проведения работ по обеспечению информационной безопасности, включая формирование экспертных групп
3	Приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 21 октября 2021 г. № 1085 «Об утверждении Административного регламента предоставления Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации государственной услуги по государственной аккредитации организаций, осуществляющих деятельность в области информационных технологий»	Требования к аккредитации организаций, осуществляющих работы в области защиты информации государственной тайны, включая экспертные группы
4	ГОСТ Р ИСО/МЭК 27004-2021. Национальный стандарт РФ. Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание»*	Требования к системам менеджмента информационной безопасности, включая оценку рисков и уязвимостей

* Приказ Росстандарта от 19 мая 2021 г. № 388-ст // СПС «КонсультантПлюс».

ния в эргасистеме сертифицированных и проверенных компонентов.

2. *Несовершенство нормативных правовых актов*. Многие страны и отрасли имеют законодательные требования и регуляторные стандарты, касающиеся защиты информации. Некоторые из них требуют проведения регулярных оценок информационной безопасности, включая базы данных. Соблюдение этих требований обязательно для соответствия закону и предотвращения штрафов или юридических последствий [6].

3. *Недостаточность защиты личных данных*. Базы данных могут содержать конфиденциальные и личные данные пользователей, клиентов или сотрудников. Оценка защиты информации помогает обнаружить уязвимости, которые могут привести к незаконному доступу к этим данным или их утечке. Это позволяет принять меры по защите конфиденциальности и личных данных, соблюдая требования закона и устанавливая доверие среди пользователей [11].

4. *Проблема доверительного взаимодействия*. Нарушение безопасности базы данных может негативно сказаться на бизнес-репутации и доверии клиентов и партнеров. Регулярная (периодическая) оценка степени защищенности привилегированной информации помогает предотвращать нарушения безопасности, минимизирует риски раскрытия конфиденциальной информации и подтверждает готовность организации защищать данные своих клиентов и партнеров [1].

В целом проведение оценки защищенности информации в базе данных информационных систем является важной мерой по обеспечению безопасности данных, соблюдению законодательных требований и защите интересов бизнеса и пользователей информационной системы. При этом одним из основных этапов оценки защищенности информации в базе данных информационной системы является сбор и анализ профессиональных экспертных оценок [8].

Существующие на данный момент системы сбора экспертных оценок обладают рядом *недостатков*, таких как отсутствие возможности детальной настройки анкеты эксперта, блокирования и удаления нерелевантных ответов в зависимости от степени согласованности экспертов, настройки сбора статистики и др. [22]. В связи с этим представляется целесообразным разработать *методические рекомендации по системному анализу* [13] экспертных оценок степени защищенности привилегированной информации в базе данных информационной системы от НСД, которые позволят устранить имеющиеся недостатки и автоматизировать проведение экспертного оценивания.

Особенности экспертного оценивания защищенности информации

При формировании экспертной группы для оценки защищенности информации рекомендуется[6] руководствоваться существующими правовыми актами и регламентами, основные из которых приведены в табл. 1. Важно заметить, что данные правовые документы предоставляют общую основу для формирования экспертной группы и проведения оценки защищенности информации. При конкретном формировании группы и проведении оценки рекомендуется дополнительно учитывать также профильные нормативные правовые акты, руководства и инструкции [17], выпущенные соответствующими регулирующими органами.

При проведении экспертной оценки принимаются меры, направленные на снижение уровня *субъективности* и *неопределенности* при определении каждой из угроз безопасности информации. В связи с этим экспертную оценку рекомендуется проводить в отношении следующих факторов [25]:

- негативного последствия от реализации угроз безопасности информации;
- целей нарушителей по реализации угроз безопасности информации;
- набора сценариев действий нарушителей при реализации угроз безопасности информации.

Оценку факторов рекомендуется проводить опросным методом с составлением анкеты, в которой указываются вопросы и возможные варианты ответа в единой принятой шкале измерений («*низкий*», «*средний*», «*высокий*» или «*да*», «*нет*», или иные шкалы). При этом вопросы должны быть четкими и однозначно трактуемыми и предполагать однозначные ответы [25].

Процесс экспертного оценивания включает, как правило, следующие основные этапы [4]:

1. Каждый эксперт проводит оценку оцениваемого параметра (рекомендуется не менее двух раундов оценки), результаты которой заносятся в таблицу.

2. После оценки каждым из экспертов отбрасываются минимальные и максимальные значения.

3. Определяется среднее значение оцениваемого параметра в каждом раунде.

4. Определяется итоговое среднее значение оцениваемого параметра.

Качественное формирование экспертной группы способствует снижению субъективных факторов при оценке угроз безопасности информации [9, 19].

Занижение (ослабление) экспертами прогнозов и предположений при оценке угроз может повлечь наступление непрогнозируемого (неожиданного) ущерба в результате их реализации. *Завышение* экспертами прогнозов и предположений при моделировании угроз безопасности информации может повлечь за собой неоправданные расходы на нейтрализацию (блокирование) угроз, являющихся неактуальными [10].

Независимо от результата формирования экспертной группы существуют субъективные факторы, связанные с особенностью процесса принятия решений при оценке степени защищенности информации в базе данных информационной системы. Это также может приводить как к занижению (ослаблению), так и к завышению (усилению) экспертами прогнозов и предположений при оценке угроз безопасности информации, что в свою очередь может привести к *пропуску* отдельных угроз безопасности информации или к неоправданным затратам на нейтрализацию неактуальных угроз. Любое решение, принимаемое экспертами при оценке угроз безопасности информации, должно исходить из *правил*, при которых нарушитель находится в наилучших условиях для реализации угрозы безопасности («*концепция гарантированной защищенности информации*» [12, 14]).

В состав экспертной группы рекомендуется включать специалистов (независимо от того, реализуются ли функции обладателя информации, заказчика и оператора в рамках одной или нескольких организаций) от подразделения, ответственного за [2]: защиту информации (обеспечение информационной безопасности); цифровую трансформацию (ИТ-специалистов); эксплуатацию сетей связи; эксплуатацию автоматизированных систем управления, а также обладателя информации или оператора, ответственного за выполнение основных (критических) процессов (бизнес-процессов). При этом специалисты должны иметь опыт работы не менее одного года по соответствующему направлению деятельности, в котором проводится оценка угроз безопасности информации [18].

Мнения экспертов часто совпадают не полностью, поэтому необходимо количественно оценивать меру согласованности экспертов и устанавливать причины несовпадения их решений. Для оценки меры согласованности мнений экспертов используются, как правило, коэффициенты конкордации (согласия) [20, 27].

Количественная мера согласованности определяется на основе статистических данных всей группы экспертов. Так, согласованность мнений компетентных экспертов при использовании всех указанных экспертных методов, где определяются ранги объектов, рассчитываются с помощью коэффициента конкордации по формуле [5]:

$$W = \frac{S}{\frac{1}{12}m^2(n^3 - n) - m\sum T_i}, \quad (1)$$

где $T_i = \frac{1}{12}\sum(t_l^3 - t^3)$ — число связок (видов повторяющихся элементов) в оценках i-го эксперта (если нет связанных рангов, то T_i равно нулю); t_l — количество элементов в l-й связке для i-го эксперта (количество повторяющихся элементов); m — число анализируемых порядковых переменных; n — количество экспертов, S — сумма квадратов отклонений, рассчитываемая по формуле (2):

[6] Методический документ «Методика оценки угроз безопасности информации» (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.).

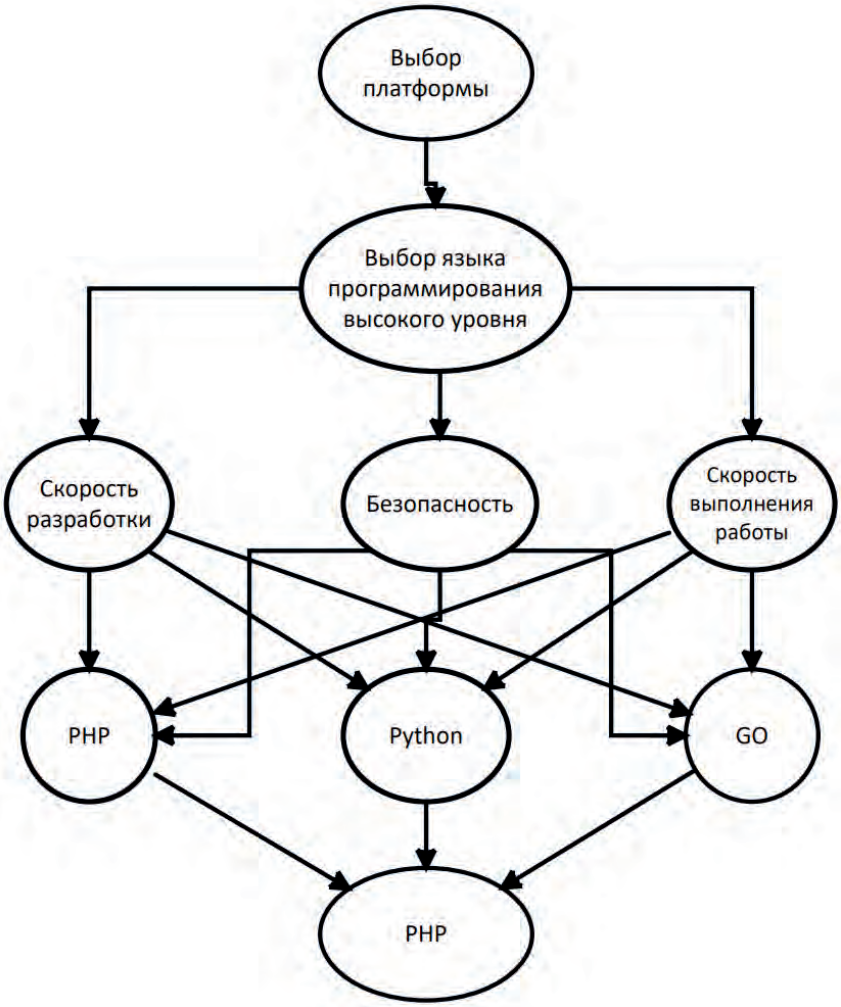

Рис. 1. Структура процесса принятия решения при выборе языка программирования высокого уровня

$$S = \sum_{i=1}^{n} r_{ij}^2 - \frac{(\sum_{i=1}^{n} r_{ij})^2}{n}, \quad (2)$$

где r_{ij} — расставленные ранги суждений группы экспертов; j — номер задания.

Эксперты должны обладать независимостью, основанной на отсутствии коммерческого и финансового интереса или другого давления, которое может оказать влияние на принимаемые решения. Не рекомендуется формировать экспертную группу из участников, находящихся в прямом подчинении, из-за возможного наличия психологического давления, так как это может негативным образом повлиять на результат определения угроз безопасности информации. В состав экспертной группы должны входить не менее трех экспертов [3].

Методические рекомендации по анализу экспертных оценок защищенности информации

При разработке методических рекомендаций были обоснованно учтены следующие основные требования и ограничения:

- возможность исключать оценки экспертов из статистики в зависимости от значения коэффициента конкордации;
- обеспечение требований кроссплатформенности;
- отсутствие территориальных ограничений при взаимодействии с приложением.

Разработанные методические рекомендации базируются на следующей логической последовательности основных этапов:

1. Обоснование платформы для создания автоматизированной системы сбора и анализа экспертной информации.
2. Разработка системы сбора и анализа экспертной информации.
3. Получение экспертной оценки.
4. Верификация полученной оценки.

На *первом* этапе реализации методических рекомендаций определяется возможный набор технологий для разработки системы сбора и анализа экспертных оценок. Для начала необходимо выбрать тип будущего приложения. Существует два основных вида — это дес-

ктопное приложение и веб-приложение [21]. В соответствии с обоснованными требованиями и принятыми ограничениями выбрана разработка веб-приложения вместо десктопного решения.

На *втором* этапе определяется основной язык программирования, используемый для веб-разработок. Одним из основных факторов определения приемлемого языка программирования является возможность поддержки созданного продукта в течение долгого периода времени. Столь же важным является наличие проверенных библиотек, которые позволят как сократить время разработки, так и повысить безопасность данного решения [23].

Выбор языка программирования высокого уровня можно осуществить с применением системы поддержки принятия решений «Выбор»[7]. На рис. 1 представлена структура процесса принятия решения при выборе приемлемого языка программирования высокого уровня с применением системологического *метода анализа иерархий* [13], включая уровень целей (определение языка программирования высокого уровня), уровень критериев (скорость разработки, безопасность, скорость выполнения программы) и уровень альтернатив (языки программирования PHP, Python, Go).

Например, скорость выполнения программы выше у языков Go и Python по сравнению с PHP. Скорость разработки и безопасность за счет большего количества проверенных библиотек выше у PHP по сравнению с Go и Python. После попарного сравнения всех критериев в программе «Выбор» было определено, что язык высокого уровня PHP набирает 0,778 балла, по сравнению с 0,145 у Python и 0,076 у Go, следовательно, язык PHP наиболее приемлем для разработки веб-приложения с обоснованными требованиями и принятыми ограничениями.

Для сокращения времени на разработку системы возможно использование фреймворка Laravel, который представляет широкий набор инструментов для быстрой и безопасной разработки. Для хранения результатов опросов в текстовом виде можно использовать (в соответствии с обоснованными требованиями и принятыми ограничениями) безопасную и быстродействующую реляционную СУБД PostgreSQL [21, 23].

Созданные опросы хранятся (рис. 2) в таблице surveys, вопросы к опросам и их части сохраняются в таблицах questions и sections. Такая схема позволяет просто добавлять и удалять вопросы в опросах. Пройденные опросы сохраняются в таблицу entries. Ответы на вопросы экспертов добавляются в таблицу answers. То есть база данных веб-приложения состоит из пяти взаимосвязанных таблиц.

Для прохождения опроса каждый эксперт должен авторизоваться на сайте. Если у эксперта нет аккаунта, он не сможет пройти опрос. Аккаунты могут создаваться как самими пользователями, так и только администратором для повышения безопасности. Вход осуществляется с помощью комбинации электронной почты и пароля.

Третий этап — получение экспертной оценки с помощью разработанной компьютерной программы. После входа в программу у каждого эксперта на экране выводится окно «Задания». В этом окне представлен перечень активных заданий. Эксперт, выбрав задание, осуществляет оценку.

Каждый добавленный опрос автоматически создает задание для всех активных экспертов. При необходимости имеется возможность выдавать задания только определенным пользователям.

В процессе выполнения одного из заданий на странице опроса эксперту достаточно в качестве оценки поставить число по 10-балльной шкале. Такой подход позволяет сократить время проведения экспертной оценки. Количество заданий, опросов и вопросов в них неограничено. Вопросы могут быть различного типа: числовые, текстовые, с одним или несколькими вариантами ответа.

В каждом опросе есть также возможность добавить проверку вводимых данных. Например, если пользователю необходимо оценить качество показателя по десятибалльной шкале, то правила валидации для ответа будут иметь следующий вид:

'rules' => [*'numeric'*, 'min:0', 'max:10'], (3)

где *'rules'* — массив правил валидации; 'numeric' — тип данных; min, max — минимальное и максимальное значение для данных типов данных соответственно.

При попытке эксперта ввести значения, выходящие за этот диапазон, система отобразит ошибку и не позволит завершить опрос. После валидации полученных ответов и завершения опроса эксперт попадает опять в личный кабинет. Завершенный опрос исчезает из заданий и считается выполненным. Каждый эксперт проходит опрос только один раз и в будущем не может изменить свои ответы.

Окно «Статистика» доступно только администратору (рис. 3).

Во вкладке «Статистика» отображается статистика по прохождению опросов: *среднее значение* каждого ответа, за исключением максимальных и минимальных значений в опросе, и *количество пользователей,* прошедших опрос. Статистика выводится в режиме реального времени. Если данных будет слишком много, есть возможность обновления статистики через определенные промежутки времени, что снизит нагрузку на базу данных. Но, как правило, экспертные команды относительно небольшие, что не создаст серьезной нагрузки на базу данных. Данные по статистике обезличены. Статистика об опросе появляется после того, как хотя бы один эксперт успешно прошел его, и выводится автоматически.

На *четвертом* этапе экспертные оценки верифицируются. Для верификации результатов оценки существует экран «Эксперты». На экране отображаются все

[7] Малтугуева Г.С., Юрин А.Ю., Дородных Н.О. Система поддержки принятия решений «Выбор» // Информационные технологии и системы. 2017. С. 163—166.

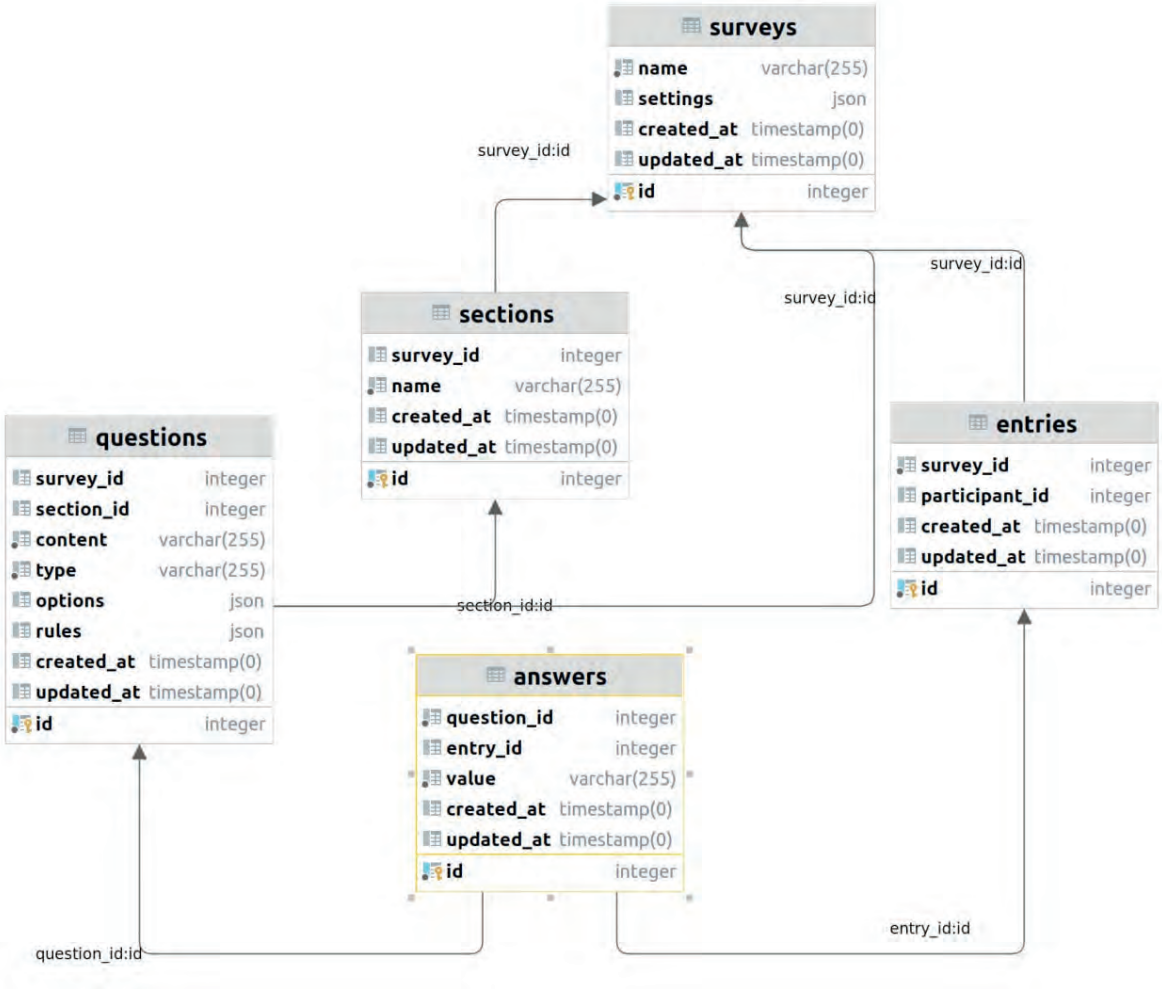

Рис. 2. Схема базы данных веб-приложения

пользователи системы (рис. 4). У каждого пользователя отображается также коэффициент согласованности. В зависимости от его значения администратор системы может принять решение о блокировании пользователя или его разблокировании. Результаты ответов экспертов с показателем конкордации, выходящим за пределы допустимых значений, установленным администратором, блокируются, и результаты их оценки не учитываются в статистике.

Численный пример

Приведем *численный пример* проведения экспертной оценки защищенности информации в информационной системе с помощью разработанных методических рекомендаций. Предположим, что необходимо провести оценку защищенности (уязвимости) информации от НСД в базе данных информационной системы. Имеется тест с пятью вопросами и пять экспертов, каждый из которых выставляет оценку от 1 до 10 баллов для каждого вопроса. Результат проведенных оценок экспертов представлен в табл. 2.

Рассчитаем число T_i связок в оценках i-го эксперта следующим образом:

$T_1 = [(2^3 — 2)]/12 = 0{,}5;$

$T_2 = [(3^3 — 3)]/12 = 2;$

$T_3 = [(2^3 — 2)]/12 = 0{,}5;$

$T_4 = [(2^3 — 2) + (2^3 — 2)]/12 = 1;$

$T_5 = [(2^3 — 2)]/12 = 0{,}5;$

$\Sigma T_i = 0{,}5 + 2 + 0{,}5 + 1 + 0{,}5 = 4{,}5.$

Так как в матрице имеются связанные ранги, произведем их переформирование. На основании переформирования рангов строится новая матрица рангов в табл. 3, используя формулу (4):

$$d = \sum r_{ij} — 15, \quad (4)$$

где $\sum r_{ij}$ — сумма рангов; 15 — сумма столбцов матрицы из табл. 3.

Исходя из матрицы рангов, сумма отклонений (S) для данных экспертов равняется 193,5.

Вычисляем коэффициент конкордации по формуле (1), используя данные из табл. 2 ($n = 5$, $m = 5$):

$$W = \frac{193.5}{\frac{1}{12}5^2(5^3 - 5) - 5 \times 4.5} = 0{,}85.$$

Название анкеты: "Защита базы данных"

Задание	Средняя оценка
1) Оцените защиту базы данных от sql-инъекций по 10 бальной шкале	4.4
2) Оцените защиту базы данных от физического проникновения по 10 бальной шкале	3.8

Количество респондентов: 5

Название анкеты: "Уязвимость информации"

Задание	Средняя оценка
1) Оцените защиту данных по 10 бальной шкале	4
2) Оцените риск прониковения в базу данных по 10 бальной шкале	5.33

Количество респондентов: 3

Название анкеты: "Оценка"

Задание	Средняя оценка
Оценка	7
Оценка	8

Количество респондентов: 2

Рис. 3. Вкладка «Статистика» в личном кабинете администратора

Активные эксперты

ФИО	Почта	Количество пройденных опросов	Оценка согласованности	Действия
Белевитин Виктор Андреевич	adamunt@mail.ru	2	0.67	Заблокировать
Иванова Диана Андреевна	adamunt2@mail.ru	1	0.67	Заблокировать

Неактивные эксперты

ФИО	Почта	Количество пройденных опросов	Оценка согласованности	Действия
Венедиктов Иван Алексеевич	dianamoiseeva56540@gmail.com	3	0.67	Разблокировать

Рис. 4. Список пользователей системы

Рассчитанное значение коэффициента конкордации $W = 0{,}85$ говорит о высокой согласованности мнений экспертов.

Рассчитаем также средний балл экспертной оценки для каждого вопроса, используя только оценки, которые остались после удаления максимальной и минимальной величин. Получаем окончательную оценку степени защищенности информации от НСД в базе данных информационной системы, усредняя средние баллы оценки экспертов по всем вопросам:

$O_c = (6{,}6 + 6{,}6 + 8{,}4 + 5 + 7{,}4) / 5 = 6{,}8$ балл.

Полученная оценка (6,8 *балл* из 10 возможных) степени защищенности информации в информационной системе — приемлемая. Эта оценка может служить показателем при сравнении степени информационной защищенности подобных систем. В дальнейшем целесообразно эту оценку использовать при анализе слабых сторон информационной системы и определения мер по ее повышению.

Заключение

Таким образом, рассмотрены результаты разработки и апробации методических рекомендаций по анализу экспертных оценок защищенности привилегированной информации в базе данных информационной системы от НСД с учетом требований существующих нормативных правовых актов в сфере информационной безопасности и необходимой степени согласованности экспертов на основе коэффициента конкордации.

Данные методические рекомендации позволяют в значительной степени сократить время сбора экс-

Таблица 3

Матрица рангов после переформирования

Факторы	Эксперты					Сумма рангов	*d*	d^2
	1	2	3	4	5			
r_{11}	3,5	3	2	1,5	3,5	13,5	-1,5	2,25
r_{21}	2	3	3	3	2	13	-2	4
r_{31}	5	5	4,5	4,5	5	24	9	81
r_{41}	1	1	1	1.5	1	5,5	-9,5	90,25
r_{51}	3,5	3	4,5	4,5	3,5	19	4	16
∑	15	15	15	15	15	75		**193,5**

пертных оценок в информационной системе за счет возможности гибкой настройки вариантов вопросов. Создание опросов для экспертов в веб-приложении позволяет уменьшить время от постановки задачи до выполнения ее экспертом. Уровень согласованности экспертов позволяет определить членов экспертной группы, которые обладают наименьшей степенью согласованности, и исключить результаты их оценки. Процесс исключения экспертов в зависимости от их коэффициента конкордации приводит к устранению нерелевантных оценок и повышает степень *достоверности* [12] общей оценки степени защищенности информации.

Встроенный интерфейс статистики позволяет в режиме реального времени анализировать полученные результаты и использовать их при оценке степени защищенности информации. Автоматизация расчета статистики также позволяет повысить *оперативность* и *экономичность* анализа экспертной информации.

Рецензент: ***Федосеев Сергей Витальевич,*** *кандидат технических наук, доцент, профессор кафедры информационного права, информатики и математики Российского государственного университета правосудия, г. Москва, Российская Федерация.*
E-mail: fedsergvit@mail.ru

Литература

1. Алексеева Ю.А., Смолькин А.С. Социальные аспекты риска: исследование риска информационных технологий // Управление рисками в экономике: проблемы и решения (РИСК'Э-2019). 2020. С. 38—41.
2. Антамошкин О.А., Пузанова Г.А., Онтужев В.В. Особенности проектирования автоматизированной системы экспертной оценки информационной безопасности организаций // Сибирский аэрокосмический журнал. 2013. № 3 (49). С. 4—8.
3. Белевитин В.А. Эффективность защиты информации на основе нечетких рисков // Мир науки без границ. 2022. С. 232—235.
4. Быков А.А., Киселева О.М., Кириллова М.А. Элементы оценки эффективности систем информационной безопасности предприятия // Труды V Юбил. Всеросс. науч.-прак. конф. с межд. участием «Вызовы цифровой экономики» (20 мая 2022 г.) / Брянский гос. инж.-технол. ун-т. Брянск : БГИТУ, 2022. С. 355—359.
5. Головань С.А., Русакова О.И. Анализ кибербезопасности в контексте современных угроз // Управленческий учет. 2022. № 10-2. С. 496—504.
6. Илларионова Т.М. Процесс нечёткого оценивания в многокритериальных экспертных оценках // Научный вестник МГТУ ГА. 2009. № 140. С. 1—3.
7. Ильин Д.Ю. Методика выбора компонентов стека технологий цифровых платформ на основе нечеткой логики // Вестник СибГУТИ. 2020. № 3 (51). С. 38—46.
8. Камалова Г.Г. Проблемы и приоритетные направления организационно-правового обеспечения конфиденциальности информации при использовании цифровых технологий // Вестник Университета им. О.Е. Кутафина. 2019. № 12 (64). С. 45—52.

9. Карасев О.И., Муканина Е.И. Метод экспертных оценок в форсайт-исследованиях // Статистика и экономика. 2019. № 4. С. 4—13.
10. Кузьмин И.Е., Баранова Е.М., Баранов А.Н., Борзенкова С.Ю. К вопросу рекомендаций оптимального качественного и количественного формирования экспертной рабочей группы для решения задач информационной безопасности // Изв. Тульского гос. ун-та. Технические науки. 2020. № 12. С. 103—107.
11. Кузьмин И.Е. Проблема значимости согласованности мнений экспертов рабочей группы при моделировании угроз безопасности информации // Изв. Тульского гос. ун-та. Технические науки. 2021. № 3. С. 254—260.
12. Ловцов Д.А. Теория защищенности информации в эргасистемах : монография. М. : РГУП, 2021. 276 с. ISBN 978-5-93916-896-0.
13. Ловцов Д.А. Системный анализ. Часть. 1. Теоретические основы. М. : РГУП, 2018. 224 с. ISBN 978-5-93916-701-7.
14. Ловцов Д.А. Проблема гарантированного обеспечения информационной безопасности крупномасштабных автоматизированных систем // Правовая информатика. 2017. № 3. С. 66—74. DOI: 10.21681/1994-1404-2017-3-66-74 .
15. Ловцов Д.А., Ермаков И.В. Классификация и модели нетрадиционных информационных каналов в эргасистеме // Науч.-техн. инф. РАН. Сер. 3. Информ. процессы и системы. 2005. № 3. С. 1—7.
16. Ловцов Д.А., Ермаков И.В. Защита информации от доступа по нетрадиционным информационным каналам // Науч.-техн. инф. РАН. Сер. 3. Информ. процессы и системы. 2006. № 9. С. 1—9.
17. Ловцов Д.А., Федичев А.В. Архитектура национального классификатора правовых режимов информации ограниченного доступа // Правовая информатика. 2017. № 2. С. 35—54. DOI: 10.21681/1994-1404-2017-2-35-54 .
18. Мамцов К.Г., Ачилов Н.Р. Киберпреступность как угроза национальной безопасности // Молодой исследователь Дона. 2022. № 1 (34). С. 42—45.
19. Милько Д.С., Данеев А.В., Горбылев А.Л. База знаний экспертной системы оценки угроз безопасности информации // Доклады Томского гос. ун-та систем управления и радиоэлектроники. 2022. Т. 25. № 1. С. 61—69.
20. Паршин И.И. Моделирование задачи определения зависимости согласованности мнения экспертов от численного состава экспертной группы // Вестник современных исследований. 2019. № 1.8 (28). С. 142—145.
21. Семенова З.В., Любич С.А., Кузнецов А.Г., Мальцев П.А. Система автоматизированной проверки правильности составления SQL-запросов: защита от уязвимостей // Динамика систем, механизмов и машин. 2017. № 4. С. 90—95.
22. Федосеев С.В. Инфологическая модель комплекса средств автоматизации компьютерных деловых игр в экспертной деятельности // Правовая информатика. 2019. № 4. С. 40—49. DOI: 10.21681/1994-1404-2019-4-40-49 .
23. Чернов А.Е. Основные требования и принципы, учитываемые при разработке и внедрении политики информационной безопасности // Вестник науки. 2023. Т. 2. № 6 (63). С. 693—699.
24. Erulanova A. et al. Expert system for assessing the efficiency of information security. 2020. 7th International Conference on Electrical and Electronics Engineering (ICEEE). IEEE, 2020. Pp. 355–359.
25. Haji S., Tan Q., Costa R.S. A hybrid model for information security risk assessment. Int. j. adv. trends comput. sci. eng. 2019. № ART-2019-111611. Pp. 100–106.
26. Schönig H.J. Mastering PostgreSQL 12: Advanced techniques to build and administer scalable and reliable PostgreSQL database applications. Packt Publishing Ltd, 2019. P. 56–67.
27. Seng L.K., Ithnin N., Said S.Z.M. The approaches to quantify web application security scanners quality: a review // International Journal of Advanced Computer Research. 2018. V. 8. No. 38. Pp. 285–312.

EXPERT EVALUATION OF INFORMATION PROTECTION IN AN INFORMATION SYSTEM DATABASE

Vladimir Alekseev, *Dr.Sc. (Technology), Professor, Head of the Department of Information Systems and Information Protection of the Tambov State Technical University, Tambov, Russian Federation.*
E-mail: vvalex1961@mail.ru

Valerii Didrikh, *Dr.Sc. (Technology), Professor at the Department of Information Systems and Information Protection of the Tambov State Technical University, Tambov, Russian Federation.*
E-mail: dve54@mail.ru

Viktor Belevitin, *Ph.D. student at the Department of Information Systems and Information Protection of the Tambov State Technical University, Tambov, Russian Federation.*
E-mail: adamunt@mail.ru

Andrei Deriabin, *Ph.D. (Technology), Associate Professor at the Department of Information Systems and Information Protection of the Tambov State Technical University, Tambov, Russian Federation.*
E-mail: 799980@mail.ru

Keywords: *information system, database, privileged information, protection, unauthorised access, expert estimate, reliability, promptness, web application, methodological recommendations, concordance coefficient, expert information.*

Abstract

Purpose of the work: increasing the reliability and promptness of expert evaluation of protection of privileged information against unauthorised access in an information system database.

Methods used in the study: system analysis, mathematical modelling and computer simulation, expert evaluation, programming.

Study findings: methodological recommendations are worked out for analysing expert estimates of protection of information against unauthorised access in an information system database considering the requirements of legal regulations in the information security field. The developed software and a justified procedure for carrying out the expert evaluation ensure the needed reliability due to the elimination of irrelevant expert estimated with a low concordance coefficient value. Using expert questionnaires in a web application which allows to reduce the time from setting the task to its fulfilment by the expert as well as the automation of the processes of gathering and processing expert information makes it possible also to increase the promptitude of the expert evaluation of information protection.

References

1. Alekseeva Iu.A., Smol'kin A.S. Sotsial'nye aspekty riska: issledovanie riska informatsionnykh tekhnologii. Upravlenie riskami v ekonomike: problemy i resheniia (RISK'E-2019), 2020, pp. 38–41.
2. Antamoshkin O.A., Puzanova G.A., Ontuzhev V.V. Osobennosti proektirovaniia avtomatizirovannoi sistemy ekspertnoi otsenki informatsionnoi bezopasnosti organizatsii. Sibirskii aerokosmicheskii zhurnal, 2013, No. 3 (49), pp. 4–8.
3. Belevitin V.A. Effektivnost' zashchity informatsii na osnove nechetkikh riskov. Mir nauki bez granits, 2022, pp. 232–235.
4. Bykov A.A., Kiseleva O.M., Kirillova M.A. Elementy otsenki effektivnosti sistem informatsionnoi bezopasnosti predpriiatiia. Trudy V Iubil. Vseross. nauch.-prak. konf. s mezhd. uchastiem "Vyzovy tsifrovoi ekonomiki" (20 maia 2022 g.), Brianskii gos. inzh.-tekhnol. un-t. Briansk : BGITU, 2022, pp. 355–359.
5. Golovan' S.A., Rusakova O.I. Analiz kiberbezopasnosti v kontekste sovremennykh ugroz. Upravlencheskii uchet, 2022, No. 10-2, pp. 496–504.
6. Illarionova T.M. Protsess nechetkogo otsenivaniia v mnogokriterial'nykh ekspertnykh otsenkakh. Nauchnyi vestnik MGTU GA, 2009, No. 140, pp. 1–3.
7. Il'in D.Iu. Metodika vybora komponentov steka tekhnologii tsifrovykh platform na osnove nechetkoi logiki. Vestnik SibGUTI, 2020, No. 3 (51), pp. 38–46.
8. Kamalova G.G. Problemy i prioritetnye napravleniia organizatsionno-pravovogo obespecheniia konfidentsial'nosti informatsii pri ispol'zovanii tsifrovykh tekhnologii. Vestnik Universiteta im. O.E. Kutafina, 2019, No. 12 (64), pp. 45–52.
9. Karasev O.I., Mukanina E.I. Metod ekspertnykh otsenok v forsait-issledovaniiakh. Statistika i ekonomika, 2019, No. 4, pp. 4–13.
10. Kuz'min I.E., Baranova E.M., Baranov A.N., Borzenkova S.Iu. K voprosu rekomendatsii optimal'nogo kachestvennogo i kolichestvennogo formirovaniia ekspertnoi rabochei gruppy dlia resheniia zadach informatsionnoi bezopasnosti. Izv. Tul'skogo gos. un-ta. Tekhnicheskie nauki, 2020, No. 12, pp. 103–107.
11. Kuz'min I.E. Problema znachimosti soglasovannosti mnenii ekspertov rabochei gruppy pri modelirovanii ugroz bezopasnosti informatsii. Izv. Tul'skogo gos. un-ta. Tekhnicheskie nauki, 2021, No. 3, pp. 254–260.
12. Lovtsov D.A. Teoriia zashchishchennosti informatsii v ergasistemakh : monografiia. M. : RGUP, 2021. 276 pp. ISBN 978-5-93916-896-0.
13. Lovtsov D.A. Sistemnyi analiz. Chast'. 1. Teoreticheskie osnovy. M. : RGUP, 2018. 224 pp. ISBN 978-5-93916-701-7.
14. Lovtsov D.A. Problema garantirovannogo obespecheniia informatsionnoi bezopasnosti krupnomasshtabnykh avtomatizirovannykh sistem. Pravovaia informatika, 2017, No. 3, pp. 66–74. DOI: 10.21681/1994-1404-2017-3-66-74 .
15. Lovtsov D.A., Ermakov I.V. Klassifikatsiia i modeli netraditsionnykh informatsionnykh kanalov v ergasisteme. Nauch.-tekhn. inf. RAN, ser. 3. Inform. protsessy i sistemy, 2005, No. 3, pp. 1–7.

16. Lovtsov D.A., Ermakov I.V. Zashchita informatsii ot dostupa po netraditsionnym informatsionnym kanalam. Nauch.-tekhn. inf. RAN, ser. 3. Inform. protsessy i sistemy, 2006, No. 9, pp. 1–9.
17. Lovtsov D.A., Fedichev A.V. Arkhitektura natsional'nogo klassifikatora pravovykh rezhimov informatsii ogranichennogo dostupa. Pravovaia informatika, 2017, No. 2, pp. 35–54. DOI: 10.21681/1994-1404-2017-2-35-54 .
18. Mamtsov K.G., Achilov N.R. Kiberprestupnost' kak ugroza natsional'noi bezopasnosti. Molodoi issledovatel' Dona, 2022, No. 1 (34), pp. 42–45.
19. Mil'ko D.S., Daneev A.V., Gorbylev A.L. Baza znanii ekspertnoi sistemy otsenki ugroz bezopasnosti informatsii. Doklady Tomskogo gos. un-ta sistem upravleniia i radioelektroniki, 2022, t. 25, No. 1, pp. 61–69.
20. Parshin I.I. Modelirovanie zadachi opredeleniia zavisimosti soglasovannosti mneniia ekspertov ot chislennogo sostava ekspertnoi gruppy. Vestnik sovremennykh issledovanii, 2019, No. 1.8 (28), pp. 142–145.
21. Semenova Z.V., Liubich S.A., Kuznetsov A.G., Mal'tsev P.A. Sistema avtomatizirovannoi proverki pravil'nosti sostavleniia SQL-zaprosov: zashchita ot uiazvimostei. Dinamika sistem, mekhanizmov i mashin, 2017, No. 4, pp. 90–95.
22. Fedoseev S.V. Infologicheskaia model' kompleksa sredstv avtomatizatsii komp'iuternykh delovykh igr v ekspertnoi deiatel'nosti. Pravovaia informatika, 2019, No. 4, pp. 40–49. DOI: 10.21681/1994-1404-2019-4-40-49 .
23. Chernov A.E. Osnovnye trebovaniia i printsipy, uchityvaemye pri razrabotke i vnedrenii politiki informatsionnoi bezopasnosti. Vestnik nauki, 2023, t. 2, No. 6 (63), pp. 693–699.
24. Erulanova A. et al. Expert system for assessing the efficiency of information security. 2020. 7th International Conference on Electrical and Electronics Engineering (ICEEE). IEEE, 2020. Pp. 355–359.
25. Haji S., Tan Q., Costa R.S. A hybrid model for information security risk assessment. Int. j. adv. trends comput. sci. eng. 2019, No. ART-2019-111611. Pp. 100–106.
26. Schönig H.J. Mastering PostgreSQL 12: Advanced techniques to build and administer scalable and reliable PostgreSQL database applications. Packt Publishing Ltd, 2019. P. 56–67.
27. Seng L.K., Ithnin N., Said S.Z.M. The approaches to quantify web application security scanners quality: a review. International Journal of Advanced Computer Research. 2018. V. 8. No. 38. Pp. 285–312.